Protection appts. against unauthorised use of commercial software - combines unique target machine ID with individual security code to produce unique password

Patent number:	DE4019652
Publication date:	1992-01-02
Inventor:	KUHN ALOIS (DE)
Applicant:	KUHN ALOIS (DE)
Classification:	
- international:	G06F12/14
- european:	G06F1/00N7R2, G06F21/00N7D
Application number:	DE19904019652 19900620
Priority number(s):	DE19904019652 19900620

Abstract of **DE4019652**

The target machine is required to have a unique "fingerprint" ID stored permanently in hardware (e.g. PROM) and accessible to software routines. When a licence is bought to run software on a partic. machine, this ID and the software licence number are communicated to the software vendor, who supplies a unique access code in return. The three values are combined by the software to produce a common internal password enables the software to run.

ADVANTAGE - Restricts use of software to designated target machines, without restricting creation of safety backup copies of purchased software.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 40 19 652 A1**

(51) Int. Cl.[6]: G 06 F 12/14

(21) Aktenzeichen: P 40 19 652.6
(22) Anmeldetag: 20. 6. 90
(43) Offenlegungstag: 2. 1. 92

(71) Anmelder:
Kuhn, Alois, 8939 Waal, DE

(74) Vertreter:
Herrmann-Trentepohl, W., Dipl.-Ing., 4690 Herne; Kirschner, K., Dipl.-Phys.; Grosse, W., Dipl.-Ing.; Bockhorni, J., Dipl.-Ing., Pat.-Anwälte, 8000 München

(72) Erfinder:
gleich Anmelder

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

US 46 85 055
EP 03 02 710 A2
EP 01 19 886 A1
EP 01 05 242 A2
DE-Z: ZELTWANGER, Holger: Kopierschutz für Programme und Zugangsschutz für Daten. In: Elektronik 17/22.8.1986, S.48-51;
- US-Z: IBM Technical Disclosure Bulletin, Vol.32, No.6A, November 1989, S.264;

(54) Verfahren zum Schutz von Software gegen unzulässiges Kopieren

(57) Zum wirksamen Schutz von Software gegen unzulässiges Kopieren wird softwareseitig ein in jedem Zielrechner anzuordnendes Rechner-Identifikations-Merkmal zur Begrenzung der Lauffähigkeit der Software auf dem jeweiligen Zielrechner genutzt. Dabei kann das Rechner-Identifikations-Merkmal mit einer Software-Lizenznummer ergänzt werden. Das um die Software-Lizenznummer ergänzte Rechner-Identifikations-Merkmal kann weiterhin mit einem Komplement komplettiert werden, so daß sich stets ein generelles softwareseitiges Paßwort ergibt.

DE 40 19 652 A1

DE 40 19 652 A1

Beschreibung

Die Erfindung betrifft ein Verfahren zum Schutz von Software gegen unzulässiges Kopieren, wenn die Software in einem entsprechenden Computer installiert ist.

Das unzulässige Kopieren von auf einem Computer installierter Software, sogenannter Originalsoftware, wird Raubkopieren genannt. Unter Raubkopieren lassen sich die unterschiedlichsten Formen der sogenannten Computer-Kriminalität zusammenfassen. Darunter fällt beispielsweise das Kopieren von Originalsoftware und Weiterverkauf auf eigene Rechnung, der Einsatz einer mit Einzellizenz erworbenen Originalsoftware auf gleichzeitig mehreren Anlagen oder das unberechtigte Kopieren von Software von Mitarbeiter und der Einsatz auf privaten Anlagen. Insgesamt sind die Erscheinungsformen des Raubkopierens unüberschaubar.

Lt. Schätzung der VSI (Vereinigung zur Förderung der Deutschen Software-Industrie) entsteht der Software-Industrie durch Raubkopieren ein Umsatzschaden von jährlich mindestens 500 Mill. DM.

Nach herrschender Meinung ist für jeden Rechner ein Originalprogramm oder eine Mehrfachlizenz für alle Computer eines Betriebes bzw. Netzes zu beziehen.

Die bisher bekannten Verfahren zum Schutz vor Raubkopieren sind zum Teil reine softwareseitige Kopierschutzmaßnahmen, die durch entsprechende Kopierprogramme übergangen werden können.

Weiterhin werden in großer Zahl kombinierte Hardware/Software-Kopierschutzmaßnahmen ergriffen. Beispielsweise ist es bekannt, auf einer Originaldiskette eine versteckte Fehlerspur anzuordnen, die bei normalem Kopieren nicht mit übertragen wird. Es wird dadurch eine sogenannte Systemdiskette gebildet, die jeweils beim Start des Programmes eingelegt werden muß.

Eine andere Art des Softwareschutzes liegt in der Festlegung und Abfragung eines Paßwortes.

Weiterhin ist eine Möglichkeit bekannt, bei der mit der Software ein sogenanntes Hardlock, also ein hardwareseitiges Schloß, mitgeliefert wird. Dieses wird an einer entsprechenden Schnittstelle des Computers angeordnet und enthält einen Speicher- oder Prozessorbaustein. Entweder wird dem Speicherbaustein eine entsprechende Kombination durch die Software entnommen oder es wird mittels eines besonderen Algorithmusses eine eingegebene Zahlenkombination modifiziert und durch die Software wieder abgefragt. Damit kann die Originalsoftware jeweils erkennen, ob der Rechner, auf dem sie gestapelt wurde, für ihren Ablauf legitimiert ist.

Alle genannten Maßnahmen haben den Nachteil gemeinsam, daß sie umgangen werden können. Weiterhin sind sie im einzelnen nicht zur Vermeidung aller Erscheinungsformen des Raubkopierens geeignet.

So kann ein Paßwortschutz nicht verhindern, daß die gleiche Software auf beliebig vielen Rechner installiert und betrieben wird, sofern der Nutzer das Paßwort kennt. Mitarbeiter eines Betriebes können somit ohne weiteres die im Dienst zur Verfügung gestellte Software auch zu Hause betreiben.

Das Anordnen von Fehlerspuren auf Originaldisketten hat sich als unsinnig erwiesen, da inzwischen gute Kopierprogramme diese Fehlerspur identisch mitübertragen.

Der Einsatz von sogenannten Hardlocks ist ebenfalls umgehbar, indem entweder durch eine entsprechende Software die Existenz des Hardlocks simuliert oder einfach das Hardlock durch Auslesen und Nachbau kopiert wird.

Weiterhin haben die bekannten Maßnahmen den Nachteil gemeinsam, daß sie auf die Software bezogen sind. Eine andere Software macht eine andere Maßnahme erforderlich.

Unter Berücksichtigung bestimmter Randbedingungen besteht also seitens der softwareproduzierenden Industrie Bedarf nach einem echten Softwareschutz für ihre Originalsoftware.

Eine Randbedingung ist dabei, daß der rechtmäßige Benutzer jederzeit die Möglichkeit haben muß, beliebig viele Sicherheitskopien seiner Originalsoftware zu erstellen. Weiterhin muß die Verwendung dieser Software auf mehreren Betriebs- oder Netzrechnern möglich sein. Möglicher organisatorischer oder verwaltungsseitiger Aufwand muß auf ein vertretbares Maß reduziert sein.

Unter Berücksichtigung der Randbedingung liegt der Erfindung die Aufgabe zugrunde, ein Verfahren zum Schutz von Software gegen Raubkopieren anzugeben, bei welchem gewährleistet ist, daß die Software nicht unberechtigterweise auf einem anderen als dem vom Software-Hersteller lizensierten Rechner ablaufen kann.

Diese Aufgabe wird durch die kennzeichnende Merkmale des Patentanspruches 1 gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen gekennzeichnet.

Dabei ist nach Maßgabe der Erfindung vorgesehen, durch Anordnen und Nutzen eines speziellen Paßwortverfahrens mit einem hardwareseitig erzeugtem Rechneridentifikations-Merkmal (RID), gleichsam einem Fingerabdruck des Rechners, die Lauffähigkeit von Software auf jedem individuellen Zielrechner zu begrenzen.

Der Lösungsvorschlag erfüllt alle in der Zielvorstellung formulierten Bedingungen. Durch Verknüpfung eines Paßwortverfahrens mit einem neu einzurichtenden Rechneridentifikationsmerkmals läßt sich ein nahezu perfekter Sortwareschutz aufbauen.

Die Rechner/Prozessoren können von den Herstellern mit einem individuellen, unzerstörbaren, unveränderbaren Identifikations-Merkmal, das über Software gelesen werden kann, ausgestattet weden. Bei diesem könnte es sich z. B. um eine mehrstellige Kombination aus Hersteller, Rechnertyp, -serie, Herstellungsdatum und laufende Nummer handeln. Sie sollte jeden produzierten Rechner eindeutig, gleich einem Fingerabdruck, identifizieren.

In Verbindung mit dieser RID kann der Software-Hersteller einen rechnerindividuellen Paßwortschutz aufbauen. Die Abarbeitung eines Programmes kann von der Eingabe eines rechnerindivuellen, vom Softwarehersteller ausgegebenen und registrierten Paßwortes abhängig gemacht werden.

Im folgenden wird die Erfindung anhand von Beispielen und Ausführungsvorschlägen sowie der Beschreibung eines möglichen organisatorischen Ablaufs erläutert.

Gemäß einem Ausführungsbeispiel kann die RID und eine Software-Lizenz-Nr. vom Softwarehersteller durch ein registriertes Rechnerpaßwort zu einem generellen Softwarepaßwort komplementiert werden.

Bei diesem Paßwortverfahren wird die mit jeder Originalsoftware ausgelieferten Softwareregistrier-Nr. (SRN) mit dem RID durch ein rechnerindividuelles Paßwort (RP) zu einem generellen Softwarepaßwort kom-

plementiert. Bei den genannten Paßwörtern sollte es sich um mehrstellige, verschlüsselte Wertekombinationen handeln, um das Erkennen von Strukturen und Gesetzmäßigkeiten soweit wie möglich zu erschweren.

Beispiel:

Software-Register-Nr. (SRN)
+ Rechneridentifikations-Merkmal
+ Rechnerindividuelles Paßwort (RP) → Komplement
= Generelles Softwarepaßwort

Das generelle Softwarepaßwort wäre somit das Schlüsselwort, durch das der Zugang zur Software eröffnet wird.

Bei dem genannten Ausführungsbeispiel handelt es sich um ein sehr stark vereinfachtes Anschauungsmodell, das von jedem Softwarehersteller beliebig erweiterbar und variierbar ist. Das generelle Softwarepaßwort kann beispielsweise, um das Erscheinungsmuster unterschiedlich zu halten, mit variablen Daten, wie Datum, Seriennummern und verschiedenen Algorithmen verschleiert werden.

Wesentlich ist bei diesem Verfahren:
Ein eindeutiges Rechneridentifikationsmerkmal, das einem rechnerindividuellen "Fingerabdruck" gleicht und hardwareseitig erzeugt wird, wird mit einem Rechnerpaßwort nach den Vorstellungen des Softwareherstellers kombiniert. Durch dieses Rechnerpaßwort kann die Lauffähigkeit von Software auf jeden einzelnen Rechner begrenzt werden. Softwarekopien wären nur noch auf dem registrierten Rechner einsetzbar.

Die Software wäre nun selbst in der Lage, vor Ausführen der eigentlichen Anwenderfunktionen die Berechtigung der Softwarebenutzung durch eine Prüfroutine wirksam zu kontrollieren und gegebenenfalls die Ausführung zu unterbinden.

Bei diesem Ausführungsbeispiel gestaltet sich die technische und organisatorische Handhabung beispielsweise wie folgt: Beim Kauf eines Software-Paketes erhält der Käufer die entsprechenden Originaldisketten mit der Angabe der Software-Registrier-Nr. (SRN). Als erster Schritt installiert der Käufer die Software mit der Installationsdiskette (SETUP-Programm). Dieses löst nach Eingabe aller Parameter das Rechner-Identifikationsmerkmal (RID) und gibt es auf den Drucker/Bildschirm aus. Der Käufer teilt dem Softwarehersteller die RID und die Software-Registrier-Nr. (SRN) mit und erhält von diesem das rechnerindividuelle Paßwort (RP) zugeteilt. Nach Eingabe dieses RP wird dieses beiden Konfigurationsdaten oder in einer speziellen Paßwortdatei gespeichert. Damit erhält dieser Rechner eine überprüfbare Nutzungsberechtigung, die erst wieder bei einer Neuinstallation durch Eingabe des RP erneuert werden müßte.

Die Originalsoftware kann zu Sicherungszwecken beliebig oft kopiert werden, kann jedoch ohne RP auf keinem anderen Rechner eingesetzt werden.

Bei Mehrfachlizenzen ist der geschilderte Vorgang für jeden Rechner zu wiederholen. Bei Netzwerklizenzen sind entsprechend alle RP von allen Netzteilnehmern abzuspeichern.

Voraussetzung ist dabei eine hardwareseitige Rechneridentifikations-Einrichtung (RIE). Bei dieser Rechner-Identifikations-Einrichtung handelt es sich um ein hardwareseitig installiertes rechnerindividuelles Merkmal — gleich einem Fingerabdruck — das unveränderbar, nicht überlagerbar und eindeutig jeden Rechner zu einem unverwechselbaren "Individuum" macht. Dieses Identifikationsmerkmal muß über Programmbefehl lesbar sein und darf nur über eine Konstante ausgegeben werden.

Das Rechner-Identifikationsmerkmal (RID) könnte ein mehrstelliger Wert mit folgendem beispielhaftem Aufbau sein.
Herstellername; -code; -kürzel
Rechnertyp;
Seriennummer;
Herstellungsdatum;
Laufende Nummer.

Daß der Rechner selbst diese Funktion integriert hat, kann natürlich erst mit neuen Herstellungsbatches realisiert werden. Dieses Verfahren könnte somit erst in Jahreszeiträumen zum Einsatz kommen. Dieses Rechner-Identifikations-Merkmal sollte in einem ROM oder PROM abgelegt sein, also nicht mehr veränderbar sein und über eine Programmanfrage als Konstante ausgegeben werden.

Zur Zeit kann nur eine externe oder zusätzliche Einheit vorgesehen werden. Dieses Verfahren kann schon mit der Auslieferung einer neuen Software-Version realisiert werden. Die neue Software-Version kann das Vorhandensein einer Ein-/Ausgabe(E/A)-Einheit RIE als Hardwarestecker an einer Schnittstelle oder als E/A-Einheit in einem freien Steckplatz erzwingen. Diese Zusatzeinrichtung würde sozusagen als "Pseudoeingabegerät" die RID liefern.

Die Rechner-Identifikations-Einrichtungen (RIE) können zudem nach Änderung der Kommunikations-Software (Protokolle) für mehr Netzsicherheit sorgen. Unerwünschte, unberechtigte Eindringlinge könnten somit sicher identifiziert und abgewiesen werden.

Patentansprüche

1. Verfahren zum Schutz vom Software gegen unzulässiges Kopieren, **dadurch gekennzeichnet,** daß softwareseitig ein in jedem Zielrechner anzuordnendes Rechner-Identifikations-Merkmal zur Begrenzung der Lauffähigkeit der Software auf jedem individuellen Zielrechner abgefragt und genutzt wird.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß ein unzerstörbar und unveränderbar in der Rechnerhardware angeordnetes Rechner-Identifikations-Merkmal genutzt wird.
3. Verfahren nach wenigstens einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß das Rechner-Identifikations-Merkmal mit einer Software-Lizenznummer ergänzt wird.
4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß das um die Softlizenznummer ergänzte Rechner-Identifikations-Merkmal softwareseitig mit einem Komplement ergänzt wird, so daß sich ein softwareseitig feststehendes generelles Paßwort ergibt.
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß softwareseitig vor Ausführen der eigentlichen Anwenderfunktionen die Berechtigung der Softwarebenutzung kontrolliert wird.

— Leerseite —